

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently Amended) An automated method of preventing an
2 endnode in a communication fabric from receiving an unauthorized
3 communication, comprising:
4 establishing a first category of management communications to include:
5 a request from a manager node to an endnode; and
6 a reply from the manager node to a request from an endnode;
7 establishing a second category of management communications to include:
8 a reply from an endnode to a request from the manager node; and
9 a request from an endnode to the manager node; and
10 at a switching device coupled to a first endnode:
11 receiving from the communication fabric a management
12 communication packet addressed to the first endnode;
13 determining whether the first endnode is a trusted endnode;
14 determining whether the management communication is a first
15 category management communication based on the management class or
16 method in which the management communication is generated; and
17 if the first endnode is not a trusted endnode, discarding the
18 management communication if the management communication is not a
19 first category management communication.
- 1 2. (Original) The method of claim 1, further comprising:

2 classifying each endnode in the communication fabric as either trusted or
3 untrusted.

1 3. (Original) The method of claim 2, wherein said classifying
2 comprises:
3 associating with each port of the switching device an indicator configured
4 to indicate whether a node coupled to the port is trusted.

1 4. (Original) The method of claim 2, wherein said classifying
2 comprises:
3 classifying the first endnode as a trusted endnode if the first endnode is a
4 manager node.

1 5. (Original) The method of claim 2, wherein said classifying
2 comprises:
3 classifying the first endnode as an untrusted endnode if the first endnode is
4 not configured to act as a manager node.

1 6. (Original) The method of claim 1, wherein said determining
2 comprises:
3 reading an indicator associated with a port of the switch to which the first
4 endnode is coupled;
5 wherein said indicator is configured to indicate whether the first endnode
6 is trusted.

1 7. (Original) The method of claim 1, further comprising, at the
2 switching device:
3 if the first endnode is trusted, forwarding the management communication

4 to the first endnode regardless of the category of the management communication.

1 8. (Original) The method of claim 1, further comprising, at the
2 switching device:
3 receiving a second management communication from the first endnode;
4 and
5 discarding the second management communication if the management
6 communication is not a second category management communication.

1 9. (Original) The method of claim 1, wherein the communication
2 fabric comprises a subnet of an InfiniBand communication fabric.

1 10. (Original) The method of claim 9, wherein a management
2 communication comprises a communication transmitted on virtual lane 15 of the
3 InfiniBand communication fabric.

1 11. (Currently Amended) A computer readable medium storing
2 instructions that, when executed by a computer, cause the computer to perform a
3 method of preventing an endnode in a communication fabric from receiving an
4 unauthorized communication, comprising:
5 establishing a first category of management communications to include:
6 a request from a manager node to an endnode; and
7 a reply from the manager node to a request from an endnode;
8 establishing a second category of management communications to include:
9 a reply from an endnode to a request from the manager node; and
10 a request from an endnode to the manager node; and
11 at a switching device coupled to a first endnode:
12 receiving from the communication fabric a management communication

13 addressed to the first endnode;
14 determining whether the first endnode is a trusted endnode;
15 determining whether the management communication is a first
16 category management communication based on the management class or
17 method in which the management communication is generated; and
18 if the first endnode is not a trusted endnode, discarding the
19 management communication if the management communication is not a
20 first category management communication.

1 12. (Currently Amended) An automated method of preventing an
2 endnode in a communication fabric from sending an unauthorized
3 communication, comprising:
4 establishing a first category of management communications to include:
5 a request from a manager node to an endnode; and
6 a reply from the manager node to a request from an endnode;
7 establishing a second category of management communications to include:
8 a reply from an endnode to a request from the manager node; and
9 a request from an endnode to the manager node; and
10 at a switching device coupled to a first endnode:
11 receiving from a first endnode a management communication addressed to
12 a second endnode in the communication fabric;
13 determining whether the first endnode is a trusted endnode;
14 determining whether the management communication is a second
15 category management communication based on the management class or
16 method in which the management communication is generated; and
17 if the first endnode is not a trusted endnode, discarding the
18 management communication if the management communication is not a
19 second category management communication.

1 13. (Original) The method of claim 12, further comprising:
2 classifying each endnode in the communication fabric as either trusted or
3 untrusted.

1 14. (Original) The method of claim 12, wherein said classifying
2 comprises:
3 associating with each port of the switching device an indicator configured
4 to indicate whether a node coupled to the port is trusted.

1 15. (Original) The method of claim 12, wherein said classifying
2 comprises:
3 classifying the first endnode as a trusted endnode if the first endnode is a
4 manager node.

1 16. (Original) The method of claim 12, wherein said classifying
2 comprises:
3 classifying the first endnode as an untrusted endnode if the first endnode is
4 not configured to act as a manager node.

1 17. (Original) The method of claim 12, wherein said determining
2 comprises:
3 reading an indicator associated with a port of the switch to which the first
4 endnode is coupled;
5 wherein said indicator is configured to indicate whether the first endnode
6 is trusted.

1 18. (Original) The method of claim 12, further comprising, at the

2 switching device:
3 if the first endnode is trusted, forwarding the management communication
4 toward the second endnode regardless of the category of the management
5 communication.

1 19. (Original) The method of claim 12, further comprising, at the
2 switching device:
3 receiving a second management communication addressed to the first
4 endnode; and
5 discarding the second management communication if the management
6 communication is not a first category management communication.

1 20. (Original) The method of claim 12, wherein the communication
2 fabric comprises a subnet of an InfiniBand communication fabric.

1 21. (Original) The method of claim 20, wherein a management
2 communication comprises a communication transmitted on virtual lane 15 of the
3 InfiniBand communication fabric.

1 22. (Currently Amended) A computer readable medium storing
2 instructions that, when executed by a computer, cause the computer to perform a
3 method of preventing an endnode in a communication fabric from sending an
4 unauthorized communication, comprising:
5 establishing a first category of management communications to include:
6 a request from a manager node to an endnode; and
7 a reply from the manager node to a request from an endnode;
8 establishing a second category of management communications to include:
9 a reply from an endnode to a request from the manager node; and

10 a request from an endnode to the manager node; and
11 at a switching device coupled to a first endnode:
12 receiving from a first endnode a management communication addressed to
13 a second endnode in the communication fabric;
14 determining whether the first endnode is a trusted endnode;
15 determining whether the management communication is a second
16 category management communication based on the management class or
17 method in which the management communication is generated; and
18 if the first endnode is not a trusted endnode, discarding the
19 management communication if the management communication is not a
20 second category management communication.

1 23. (Currently Amended) An apparatus for preventing a node in a
2 communication fabric from engaging in unauthorized communication, the
3 apparatus comprising:
4 a switching device configured to route management communications
5 through the communication fabric, wherein:
6 a type one management communications comprise requests from a
7 manager node to endnodes and replies from the manager node to requests
8 from endnodes; and
9 a type two management communications comprise replies from
10 endnodes to requests from the manager node and requests from
11 endnodes to the manager node;
12 wherein a management communication is categorized to be a type
13 one or a type two management communication based on the management
14 class or method in which the management communication is generated;
15 for each port of the switching device, an indicator configured to indicate
16 whether an endnode coupled to the port is trusted;

17 wherein a first management communication addressed to a first endnode
18 coupled to a first port of the switching device is discarded if the first endnode is
19 not trusted and the first management communication is not a type one
20 management communication; and

21 wherein a second management communication received from the first
22 endnode is discarded if the first endnode is not trusted and the second
23 management communication is not a type two management communication.

1 24. (Original) The apparatus of claim 23, further comprising:
2 a secure channel configured to allow a management node to configure said
3 indicators.

1 25. (Original) The apparatus of claim 23, wherein:
2 for each port coupled to another switching element, said indicator is set to
3 indicate the other switching element is trusted.

1 26. (Original) The apparatus of claim 23, wherein:
2 for each port coupled to a management node, said indicator is set to
3 indicate the management node is trusted.

1 27. (Original) The apparatus of claim 23, wherein:
2 for each port coupled to an endnode that is not configured to act as a
3 management node, said indicator is set to indicate the endnode is not trusted.

1 28. (Original) The apparatus of claim 23, wherein:
2 the communication fabric comprises an InfiniBand communication fabric;
3 and
4 a management communication comprises a communication transmitted

5 over virtual lane 15 of the InfiniBand communication fabric.

1 29. (Currently Amended) A computer readable medium residing in a
2 communication switch and containing a data structure configured for indicating
3 trust, the data structure comprising:

4 for each port of the communication switch, an indicator configured to
5 indicate whether a communication node coupled to the port is trusted;

6 wherein a port indicator is set to a first state if the coupled communication
7 node is trusted and is set to a second state if the coupled communication node is
8 not trusted; and

9 wherein management communications addressed to the coupled
10 communication node are filtered based on the management class or method in
11 which the management communications are generated if the port indicator is set to
12 said second state.